IN THE CLAIMS

This listing of claims replaces are prior listings:

1. (Currently Amended) A person authentication system for executing person authentication by comparing a template which is previously acquired person identification data with sampling information input by a user, said system comprising:

a person identification authority which creates a person identification certificate for storing the template and which issues the person identification certificate to an entity which executes person authentication,

wherein

said person identification authority acquires the template and data for person identification from the user to be certified with the person identification certificate, and encrypts the template using a public key and creates and registers, on the basis of the identification of the user, the person identification certificate for storing the encrypted template which is the person identification data,

the entity which decrypts the encrypted template stored in the person identification certificate and executes person authentication compares the decrypted template with the sampling information of the user so as to execute person authentication, and

the public key used to encrypt or decrypt the template stored in the person identification certificate being a different public key depending upon the entity which executes authentication of a person.

2. (Original) The system according to claim 1, wherein said person identification authority acquires a template deleting request and the data for person identification from the user to be certified with the person identification certificate, deletes the template from the person identification certificate, and registers the person identification certificate in a revocation list, on the basis of the identification of the user.

3. (Original) The system according to claim 1, wherein said person identification authority acquires a new template and the data for person identification together with a template changing request from the user to be certified with the person identification certificate, deletes an old template from the person identification certificate, deletes the person identification certificate for storing the old template, registers the person identification certificate in the revocation list, and creates and registers a person identification certificate for storing the new template, on the basis of the identification of the user.

4. (Original) The system according to claim 1, wherein said person identification authority acquires an additional template and the data for person identification together with a template addition request from the user to be certified with the person identification certificate, and creates and registers a person identification certificate for storing the additional template as well as the template of the user on the basis of the identification of the user.

5. (Original) The system according to claim 1, wherein said person identification authority acquires the data for person identification together with a template suspension request from the user to be certified with the person identification certificate, invalidates the template stored in the person identification certificate, and registers the person identification certificate in the revocation list, on the basis of the identification of the user.

6. (Original) The system according to claim 1, wherein said person identification authority acquires the data for person identification together with a template suspension cancel request from the user to be certified with the person identification certificate, re-validates the template stored in the person identification certificate, and erases the person identification certificate from the revocation list, on the basis of the identification of the user.

7. (Original) The system according to claim 1, wherein said person identification authority executes mutual authentication with a user device, in data communication with the user device performed when the user to be certified with the person identification certificate requests registration, deletion, change, addition, suspension, or canceling of suspension of the template, and prevents and verifies data-tampering by creating a digital signature and performing signature verification.

8. (Original) The system according to claim 1, wherein said person identification authority issues, in response to a request from the entity which executes person authentication, the registered person identification certificate to the entity, and in the issuing of the person identification certificate to the entity, the template to be stored in the person identification certificate is issued as an encrypted data which may be decrypted in the entity.

9. (Original) The system according to claim 1, wherein said person identification authority issues, in response to a request from the entity which executes person authentication, the registered person identification certificate to the entity, and in the issuing of the person identification certificate to the entity, the template to be stored in the person identification certificate is issued as data encrypted with a public key of the entity.

10. (Original) The system according to claim 1, wherein said person identification authority updates, in response to a request from the entity which executes person authentication, the person identification certificate previously issued to the entity, and in the updating of the person identification certificate to the entity, a new person identification certificate of which validity is reset is issued to the entity.

11. (Original) he system according to claim 1, wherein said person identification authority acquires a request for deleting the person identification certificate and the data for person identification from the user to be certified with the person identification certificate, deletes the person identification certificate, and requests deletion of the issued person identification certificate to the entity to which the person identification certificate is issued, on the basis of the identification of the user.

12. (Original) he system according to claim 1, wherein said person identification authority performs comparison for verification based on the person identification certificate in response to a request from the entity which executes person authentication, and in the comparison for verification of the person identification certificate to the entity, the sampling information received from the entity is compared with the template in the person identification certificate stored in said person identification authority, and a comparison result is provided as a response to the entity.

13. (Original) The system according to claim 1, wherein said person identification authority executes mutual authentication with a device of the entity, in data communication with the entity performed to issue, update, delete, or inquire the person identification certificate to the entity which executes person authentication, and verifies data validity by checking whether the data is tampered with by adding the digital signature and performing signature verification.

14. (Previously Amended) The system according to claim 1, wherein the template to be stored in the person identification certificate created by said person identification authority comprises biometric information of a person selected from the group consisting of fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; non-biometric information selected from the group consisting of a seal impression, a passport, a driver's license, and a credit card; any combination of two or more of the biometric information and the non-biometric information; or a combination of any of the biometric or non-biometric information and a password.

15. (Original) The system according to claim 1, wherein the person identification certificate issued by said person identification authority includes the digital signature written by said person identification authority.

16. (Previously Amended) The system according to claim 1, wherein the entity is a service provider which provides services to the user identified by the person identification certificate, a user device that the user identified by the person identification certificate accesses, or said person identification authority.

17.   (Currently Amended) A person authentication method for executing person authentication by comparing a template which is previously acquired person identification data with sampling information input by a user, said method comprising the steps of:

creating a person identification certificate for storing the template and issuing the person identification certificate to an entity which executes person authentication in a person identification authority,

acquiring the template and data for person identification from the user to be certified with the person identification certificate, and encrypting the template using a public key and creating and registering, on the basis of the identification of the user, the person identification certificate for storing the encrypted template which is the person identification data, and

decrypting the encrypted template and comparing the decrypted template with the sampling information of the user so as to execute person authentication in the entity which executes person authentication, the public key used to encrypt or decrypt the template stored in the person identification certificate being a different public key depending upon the entity which executes authentication of a person.

18.   (Original)   The method according to claim 17, wherein said person identification authority acquires a template deleting request and the data for person identification from the user to be certified with the person identification certificate, deletes the template from the person identification certificate, and registers the person identification certificate in a revocation list, on the basis of the identification of the user.

19.   (Original)   The method according to claim 17, wherein said person identification authority acquires a new template and the data for person identification together with a template changing request from the user to be certified with the person identification certificate, deletes an old template from the person identification certificate, deletes the person identification certificate for storing the old template, registers the person identification certificate in the revocation list, and creates and registers a person identification certificate for storing the new template, on the basis of the identification of the user.

20. (Original)   The method according to claim 17, wherein said person identification authority acquires an additional template and the data for person identification together with a template addition request from the user to be certified with the person identification certificate, and creates and registers a person identification certificate for storing the additional template as well as the template of the user on the basis of the identification of the user.

21. (Original)   The method according to claim 17, wherein said person identification authority acquires the data for person identification together with a template suspension request from the user to be certified with the person identification certificate, invalidates the template stored in the person identification certificate, and registers the person identification certificate in the revocation list, on the basis of the identification of the user.

22. (Original)   The method according to claim 17, wherein said person identification authority acquires the data for person identification together with a template suspension cancel request from the user to be certified with the person identification certificate, re-validates the template stored in the person identification certificate, and erases the person identification certificate from the revocation list, on the basis of the identification of the user.

23. (Original)   The method according to claim 17, wherein said person identification authority executes mutual authentication with a user device, in data communication with the user device performed when the user to be certified with the person identification certificate requests registration, deletion, change, addition, suspension, or canceling of suspension of the template, and prevents and verifies data-tampering by creating a digital signature and performing signature verification.

24. (Original)   The method according to claim 17, wherein said person identification authority issues, in response to a request from the entity which executes person authentication, the registered person identification certificate to the entity, and in the issuing of the person identification certificate to the entity, the template to be stored in the person identification certificate is issued as an encrypted data which may be decrypted in the entity.

25. (Original)   The method according to claim 17, wherein said person identification authority issues, in response to a request from the entity which executes person authentication, the registered person identification certificate to the entity, and in the issuing of the person identification certificate to the entity, the template to be stored in the person identification certificate is issued as data encrypted with a public key of the entity.

26. (Original)   The method according to claim 17, wherein said person identification authority updates, in response to a request from the entity which executes person authentication, the person identification certificate previously issued to the entity, and in the updating of the person identification certificate to the entity, a new person identification certificate of which validity is reset is issued to the entity.

27. (Original)   The method according to claim 17, wherein said person identification authority acquires a request for deleting the person identification certificate and the data for person identification from the user to be certified with the person identification certificate, deletes the person identification certificate, and requests deletion of the issued person identification certificate to the entity to which the person identification certificate is issued, on the basis of the identification of the user.

28. (Original)   The method according to claim 17, wherein said person identification authority performs comparison for verification based on the person identification certificate in response to a request from the entity which executes person authentication, and in the comparison for verification of the person identification certificate to the entity, the sampling information received from the entity is compared with the template in the person identification certificate stored in said person identification authority, and a comparison result is provided as a response to the entity.

29.   (Original)   The method according to claim 17, wherein said person identification authority executes mutual authentication with a device of the entity, in data communication with the entity performed to issue, update, delete, or inquire the person identification certificate to the entity which executes person authentication, and verifies data validity by checking whether the data is tampered with by adding the digital signature and performing signature verification.

30.   (Currently Amended) A program providing medium for providing a computer program which executes person authentication in a computer system by comparing a template which is previously acquired person identification data with sampling information input by a user, said computer program comprising the steps of:

acquiring the template and data for person identification from the user to be certified with a person identification certificate,

encrypting the template using a public key,

creating and registering, on the basis of the identification of the user, the person identification certificate for storing the encrypted template which is the person identification data, and

decrypting the encrypted template and comparing the decrypted template with the sampling information of the user so as to execute person authentication in the entity which executes person authentication, the public key used to encrypt or decrypt the template stored in the person identification certificate being a different public key depending upon the entity which executes authentication of a person